



*El placer de cautivar y crear nuevos mercados*

# IBM Security

Intelligence. Integration. Expertise.

## Steve Robinson

VP Development, Strategy and Product Management

IBM Security Systems Division

# Please note:

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

# The Journey Toward a Smarter Planet Continues

Smart Supply Chains



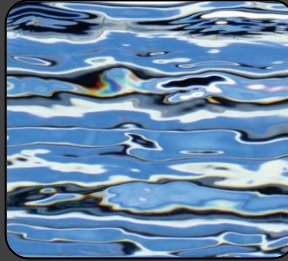
Smart Countries



Smart Retail



Smart Water Management



Smart Weather



Smart Energy Grids



INSTRUMENTED



INTERCONNECTED



INTELLIGENT

Smart Oil Field Technologies



Smart Regions



Smart Healthcare



Smart Traffic Systems

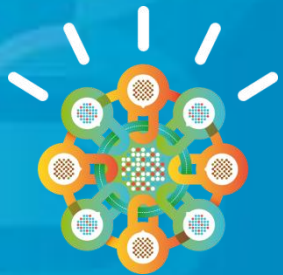


Smart Cities



Smart Food Systems



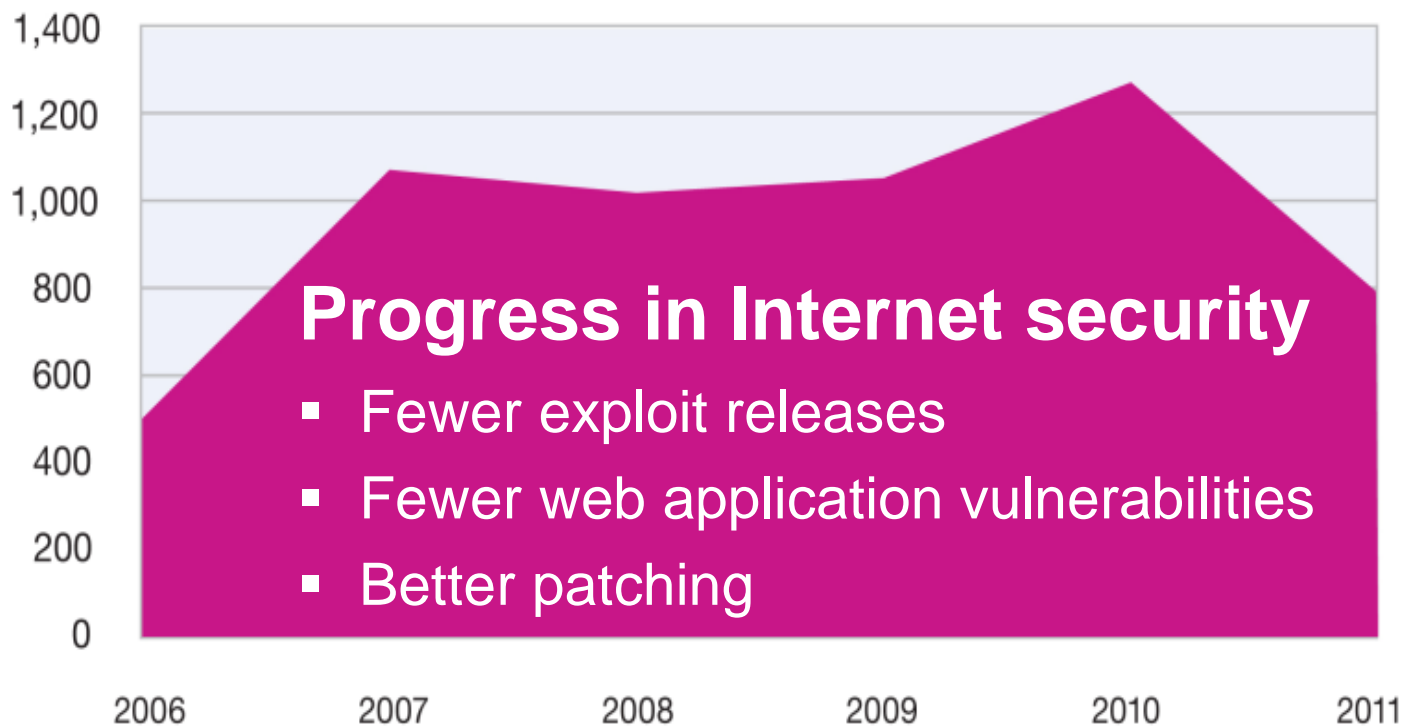


# Security Threats Are Accelerating



# Key Findings from the 2011 IBM X-Force® Trend & Risk Report

## Public Exploit Disclosures 2006-2011



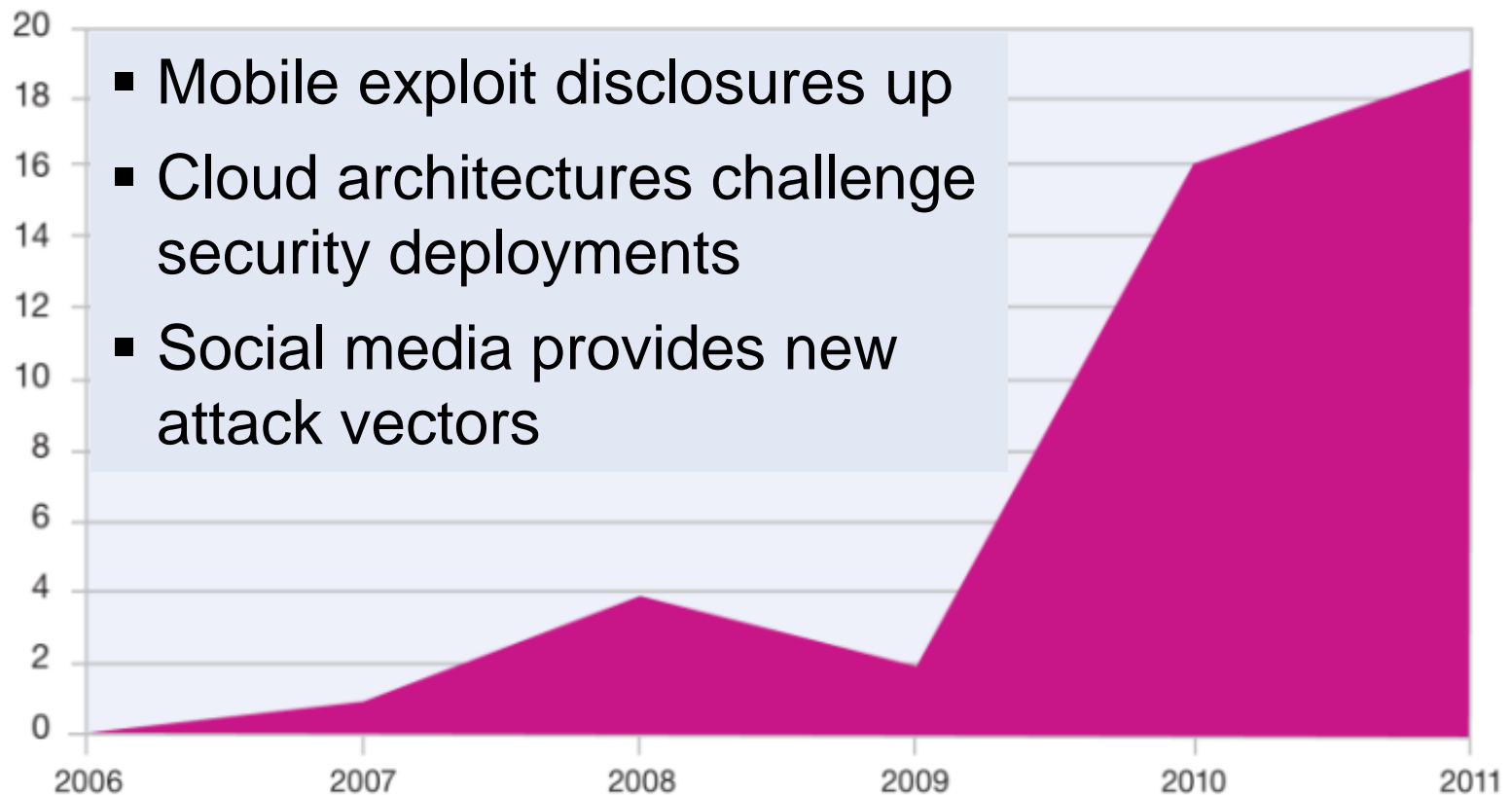
### Progress in Internet security

- Fewer exploit releases
- Fewer web application vulnerabilities
- Better patching

**But...**

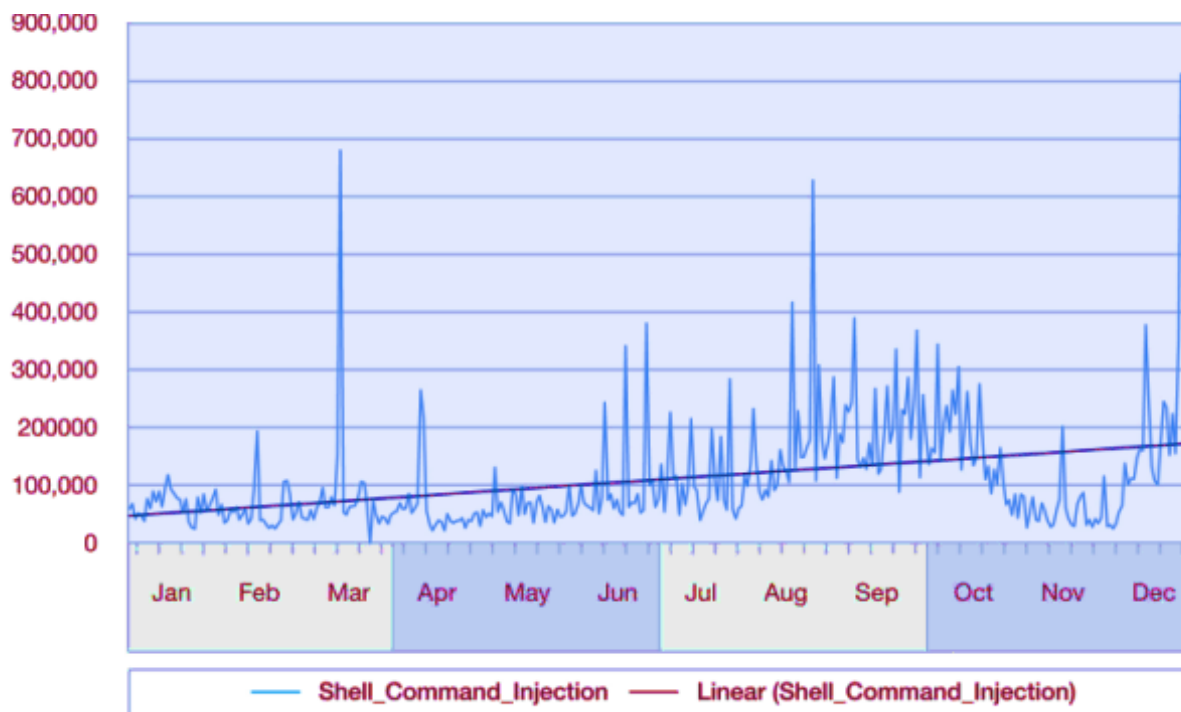
# New technologies present new challenges

## Mobile Operating System Exploits 2006-2011



# Attack sophistication is on the rise

## Top MSS High Volume Signatures & Trend Line Shell Command Injection 2011



- Shell Command Injection attacks are up
- Spikes in SSH Brute Forcing
- Increase in phishing based malware distribution and 'click' fraud





## Business Results

Sony estimates potential \$1B long term impact – \$171M / 100 customers

## Brand Image

HSBC data breach discloses 24K private banking customers

## Supply Chain

Epsilon breach impacts 100 national brands

## Legal Exposure

TJX estimates \$150M class action settlement in release of credit / debit card info

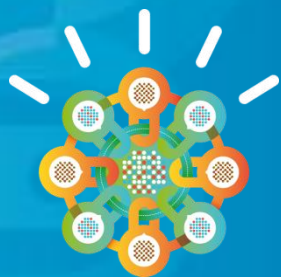
## Impact of hacktivism

Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony ...

## Audit Risk

Zurich Insurance PLC fined £2.275M (\$3.8M) for the loss and exposure of 46K customer records

# IT Security Is a Board Room Discussion



# **Clients Face Complex Security Challenges**

# Who is attacking our networks?

## Attacker Types and Techniques 2011 H1

### Off-the-Shelf tools and techniques

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS



### Sophisticated

- Cyberwar

**Broad**

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)



- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

**Targeted**

# Advanced Persistent Threat (APT) Is Different

## 1 Advanced

- Exploiting unreported vulnerabilities
- Advanced, custom malware not detected by antivirus products
- Coordinated, researched attacks using multiple vectors

## 2 Persistent

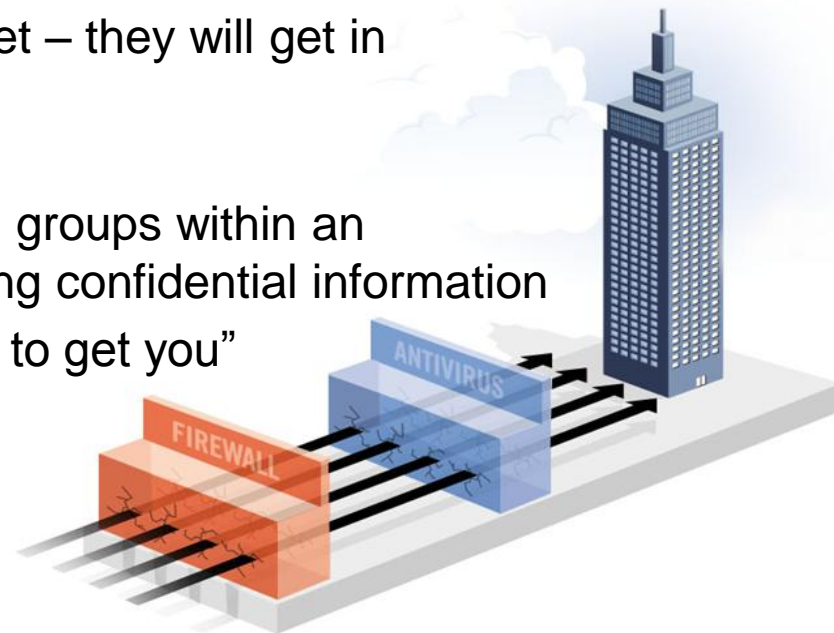
- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in

## 3 Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are “out to get you”

## 4 Watch, Wait, Plan

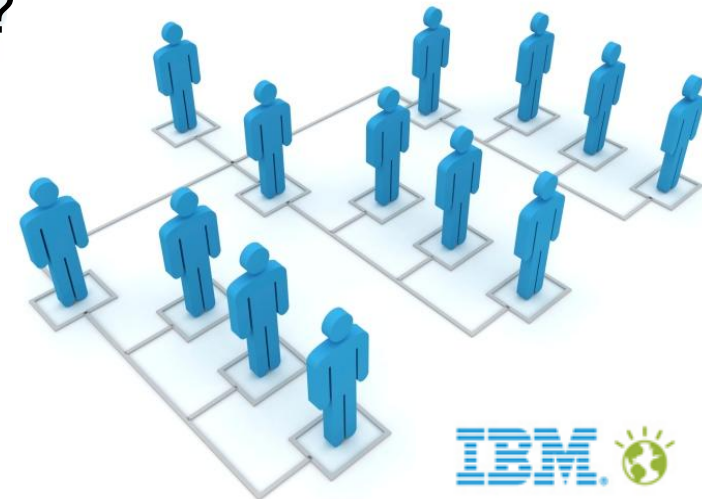
- Responding is different too – call for help





# Internet Intelligence Collection

- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?
- Search for LinkedIn, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart
- Who works with the information we want to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?

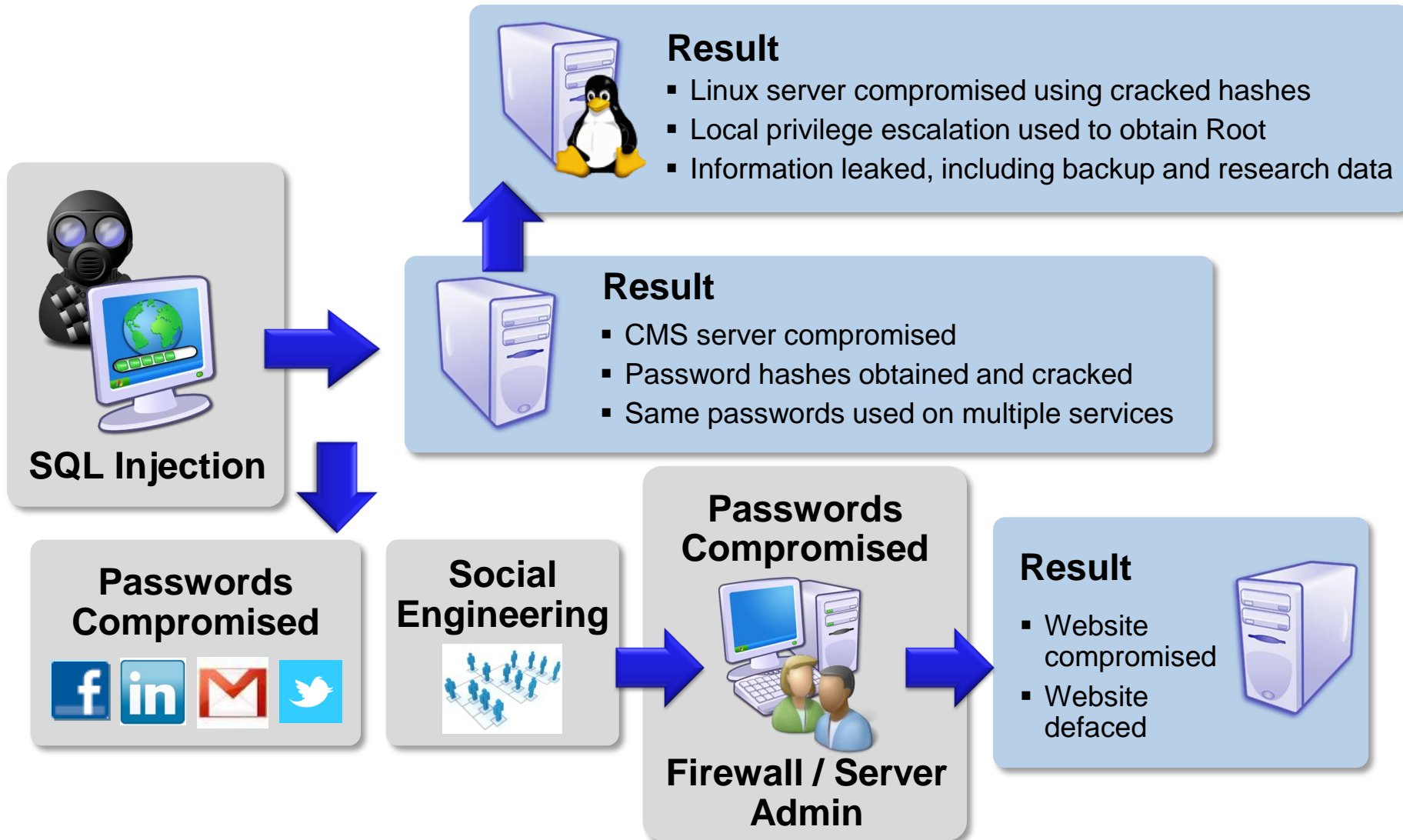




Well known, basic attack techniques are all that it takes: *Anatomy of an APT – Scenario 1*



# Well known, basic attack techniques are all that it takes: *Anatomy of an APT – Scenario 1*



# There are many ways to stop an attack

## SQL Injection



SQL Injection

- Blocked by IPS
- Discovered by AppScan before attack

## Poor password hashing



- Discovered by VA scan or security audit

## Privilege escalation Secure Shell Host (SSH)



- Patch management to fix privilege escalation

## Passwords compromised



- User training / education about sharing credentials between sites

# They Will Get In...Then What? *Anatomy of an APT – Scenario 2*

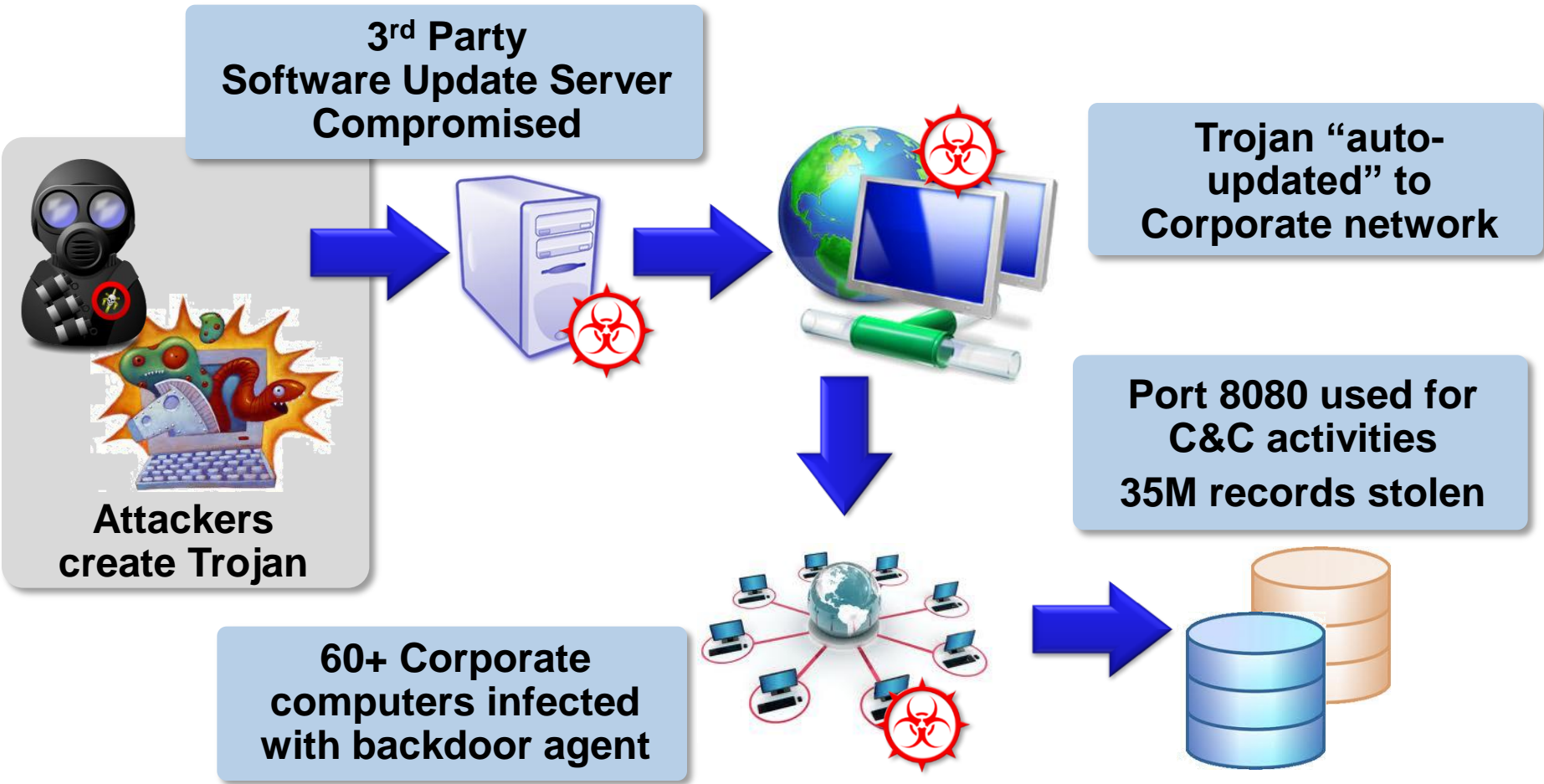


**Attackers  
create Trojan**



**Attackers  
create Trojan**

# They Will Get In... Then What? *Anatomy of an APT – Scenario 2*



**-6 Months**      **Day 0**      **Day 8**



# An attack will happen... You need Security Intelligence

**3rd party software update server compromised**



- Business Partner security

**60+ corporate computers infected with backdoor agent**

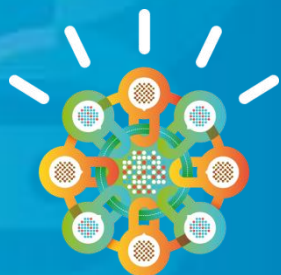


- Recon detection

**Port 8080 used for C&C activities  
35M records stolen**

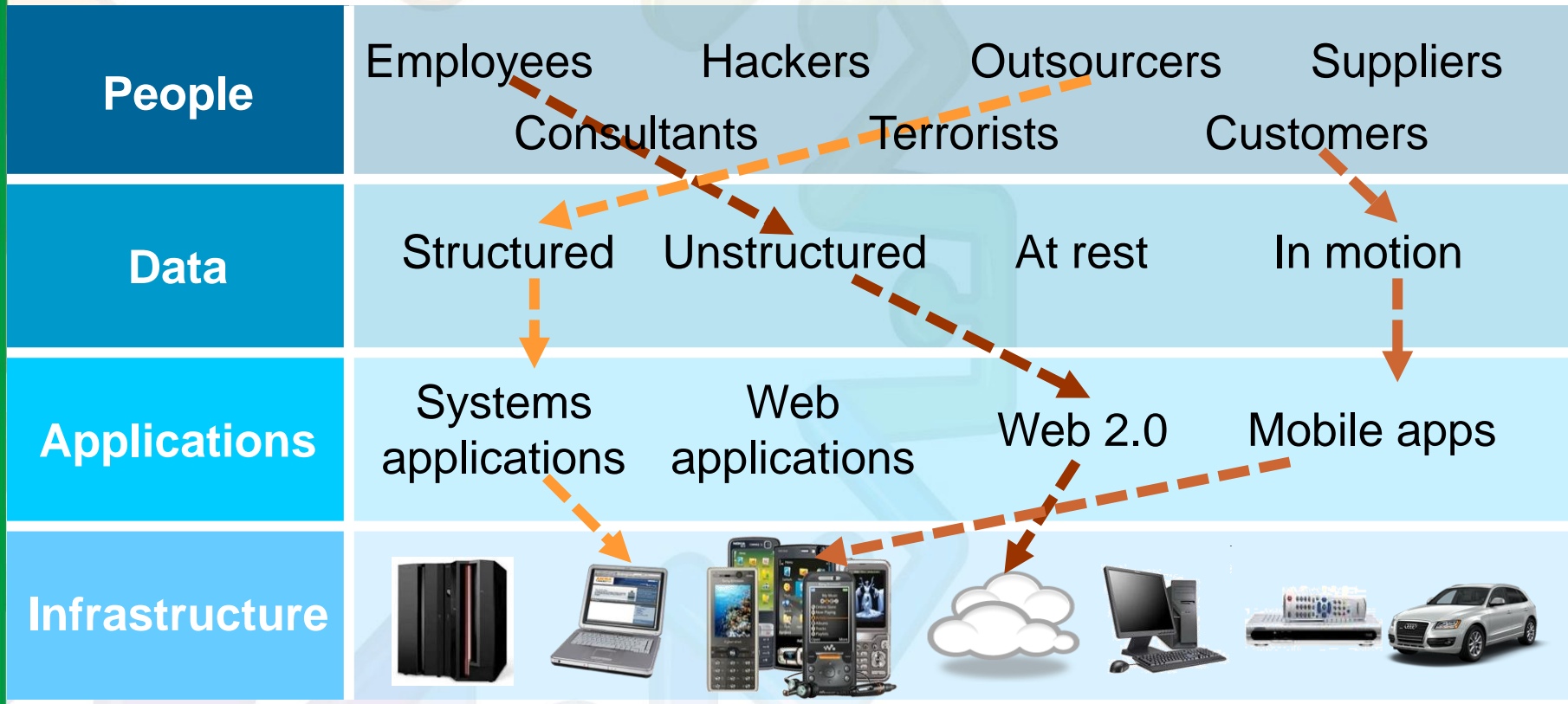


- Anomaly detection
- Database monitoring and protection



# IBM's Security Strategy

# Solving a security issue is a complex, four-dimensional puzzle



Attempting to protect the perimeter is not enough – siloed point products cannot adequately secure the enterprise

# IBM Security: Think Integrated. Think Intelligent.

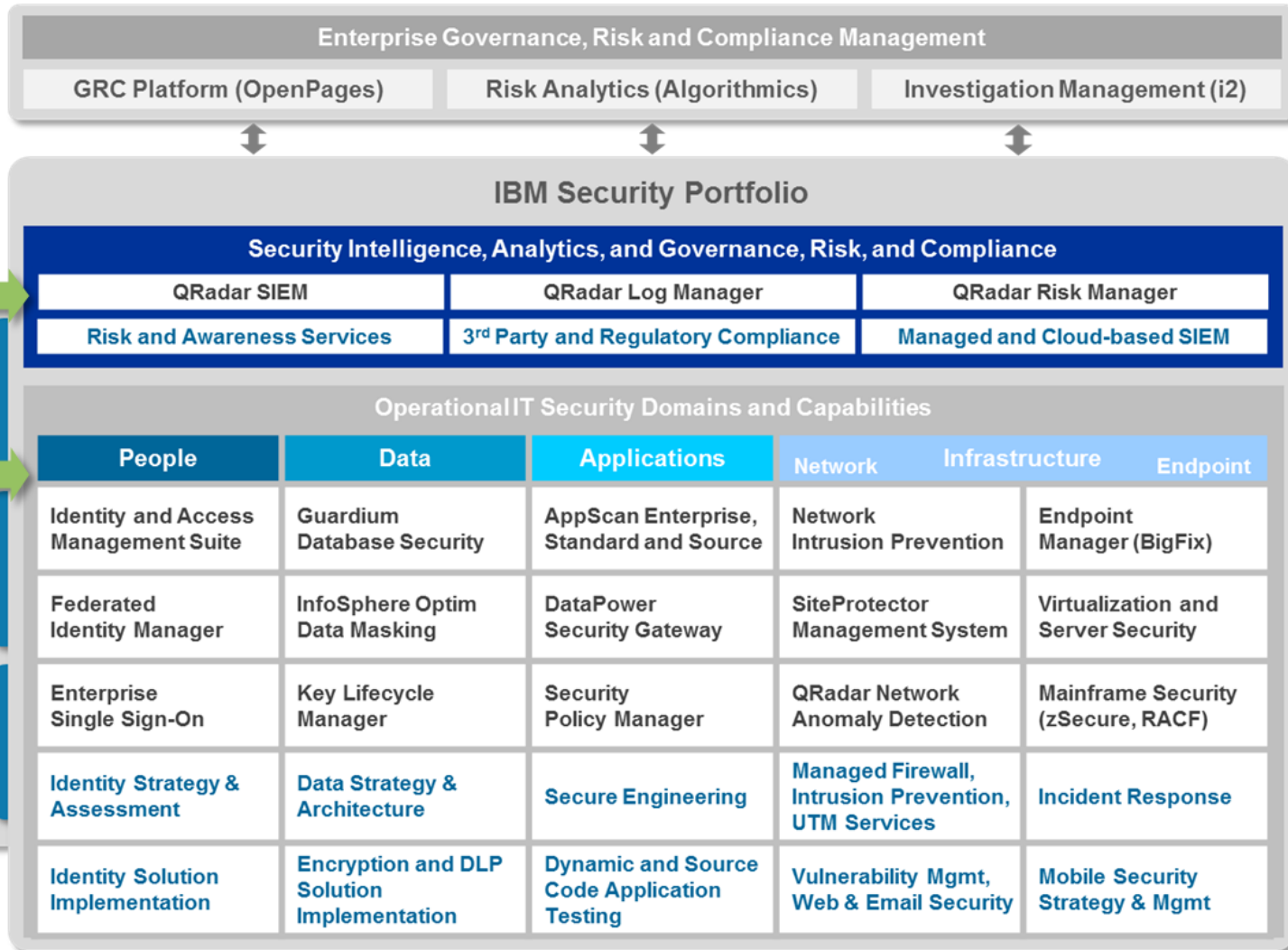
## IBM Security Systems

- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force<sup>®</sup> research
- One of the largest vulnerability databases



**Intelligence • Integration • Expertise**

# Intelligence: A comprehensive portfolio of products and services across all domains



Security Ecosystem

Partner Programs (3<sup>rd</sup> party)

Standards

Security Consulting

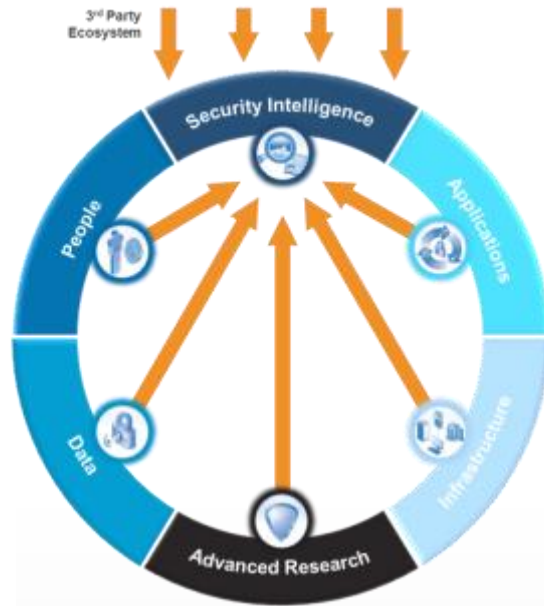
Managed and Cloud Services

X-Force and IBM Research



# Integration: Increased security, collapsed silos, reduced complexity

## Integrated Intelligence.



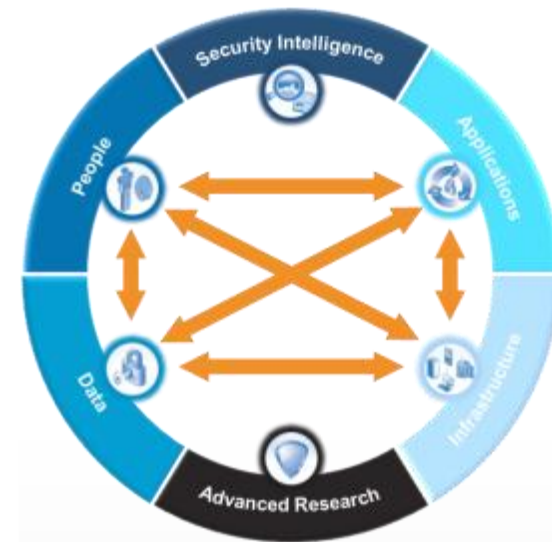
- Advanced analytics
- Detection, notification and response
- Automation and risk assessment

## Integrated Research.



- Identify threats
- Detect vulnerabilities
- Add security intelligence

## Integrated Protection.



- Customize protection
- Converge access management with web service gateways
- Link identity information with database security

# Expertise: Global coverage and security awareness



- Security Operations Centers
- Security Research Centers
- Security Solution Development Centers
- Institute for Advanced Security Branches




**IBM Research**



**IBM Institute for Advanced Security**  
Enabling cybersecurity innovation and collaboration

**14B** analyzed Web pages & images  
**40M** spam & phishing attacks  
**54K** documented vulnerabilities  
**Billions** of intrusion attempts daily  
**Millions** of unique malware samples



**World Wide Managed Security Services Coverage**

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)



**How is IBM helping solve complex security challenges?**

# How do we help with today's security mega-trends?

## Security Intelligence 1



Enterprise Customers



## Cloud Computing 2



## Advanced Threats 3



Advanced Persistent Threats  
Stealth Bots • Targeted Attacks  
Designer Malware • Zero-days

## Mobile Computing 4



## Identity 5



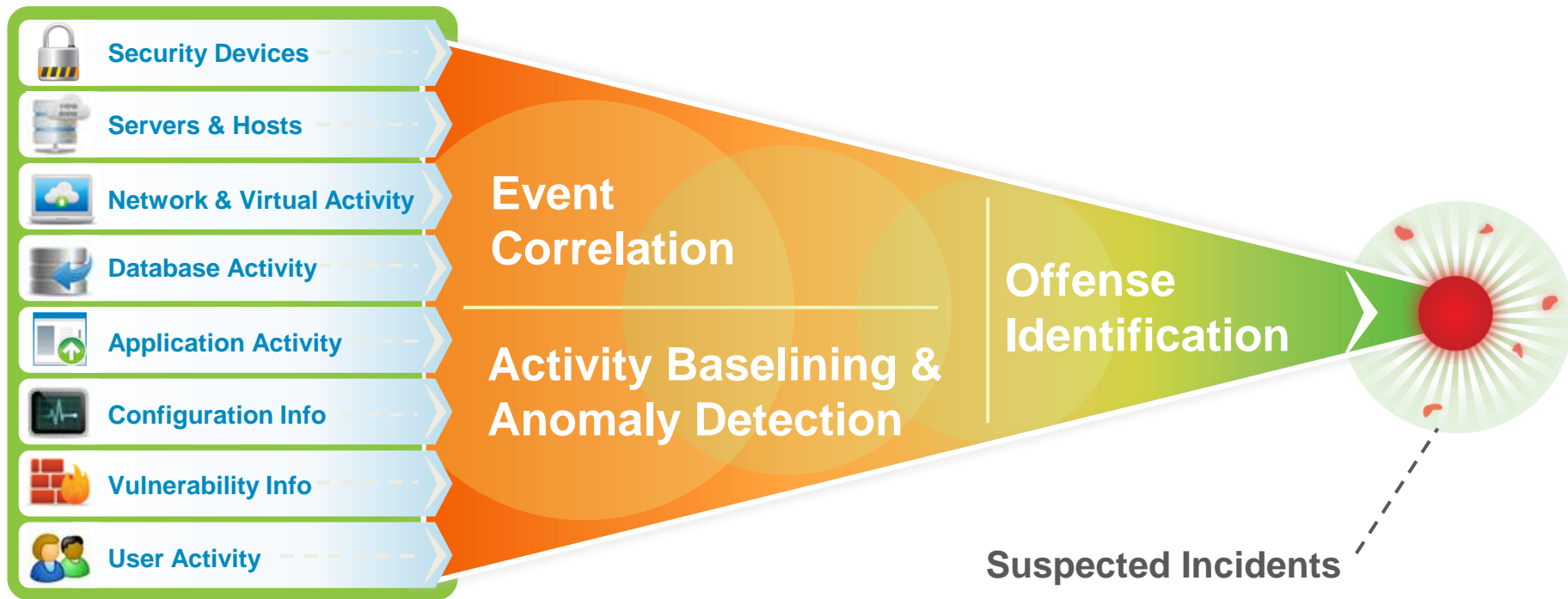
## Regulation/Compliance 6





# Security Intelligence:

*Integrating across IT silos with Security Intelligence solutions*



Extensive Data Sources

+

Deep Intelligence

=

Exceptionally Accurate and Actionable Insight



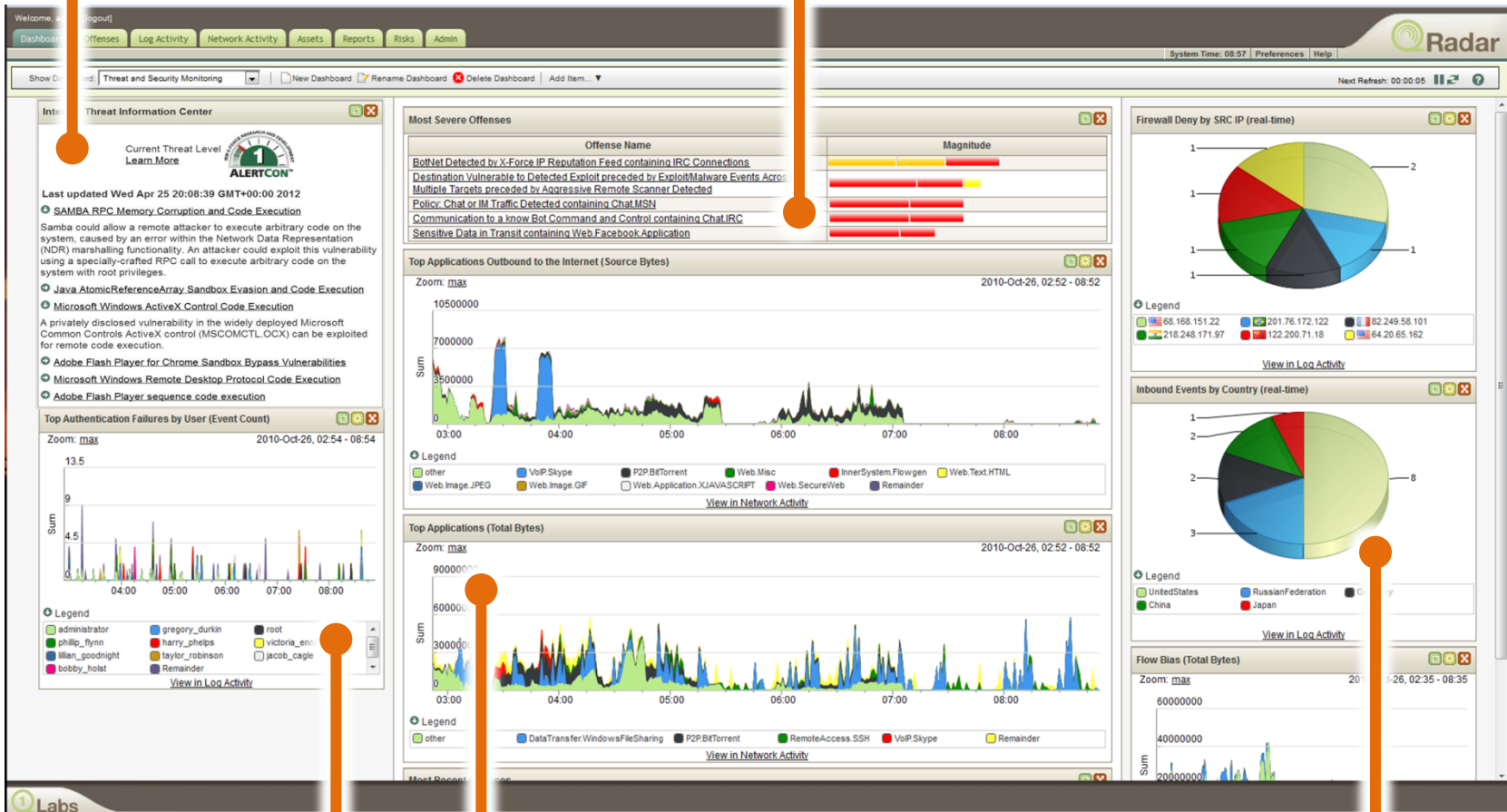


# Security Intelligence: *QRadar provides security visibility*



## IBM X-Force® Threat Information Center

## Real-time Security Overview w/ IP Reputation Correlation



Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

# Cloud: *Our focus is in two areas of cloud security*

## 1 Security from the Cloud

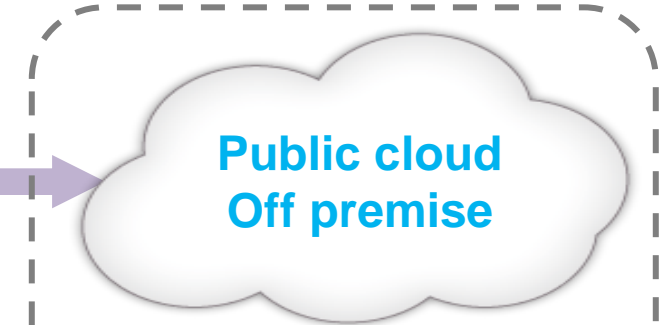


Use cloud to deliver security **as-a-Service** - focusing on services such as vulnerability scanning, web and email security, etc.



Securing the Private Cloud stack – focusing on building security into the cloud infrastructure and its workloads

## 2 Security for the Cloud



Secure usage of Public Cloud applications – focusing on Audit, Access and Secure Connectivity



# Cloud: Leverage solutions in each area of cloud risk



## IBM Identity and Access Management Suite

Identity integration, provision users to SaaS applications  
Desktop single sign on supporting desktop virtualization



## IBM QRadar Security Intelligence

Total visibility into virtual and cloud environments



## IBM AppScan Suite

Scan cloud deployed web services and applications for vulnerabilities



## Securing Cloud with IBM Security Systems

Security Intelligence • People • Data • Apps • Infrastructure



## IBM InfoSphere Guardium Suite

Protect and monitor access to shared databases



## IBM Network IPS

Protect and monitor access to shared databases



## IBM Endpoint Manager

Patch and configuration management of VMs

## IBM Virtual Server Protection for VMware

Protect VMs from advanced threats

# Advanced Threat: *The challenging state of network security*



Stealth Bots • Targeted Attacks  
Worms • Trojans • Designer Malware

## SOPHISTICATED ATTACKS

Increasingly sophisticated attacks are using multiple attack vectors and increasing risk exposure



## STREAMING MEDIA

Streaming media sites are consuming large amounts of bandwidth



## SOCIAL NETWORKING

Social media sites present productivity, privacy and security risks including new threat vectors

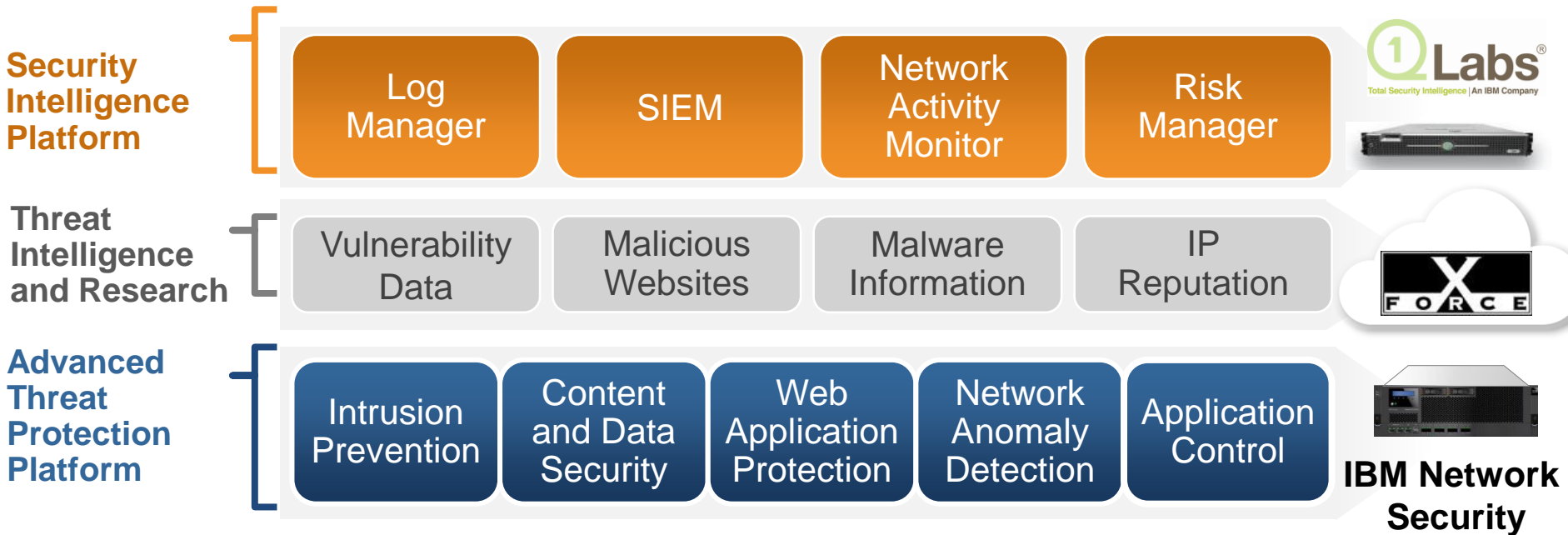


URL Filtering • IDS / IPS  
IM / P2P • Web App Protection  
Vulnerability Management

## POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

# Advanced Threats: *IBM's vision for Threat*



## Advanced Threat Protection Platform

- Leverage extensible set of network security capabilities
- Granular application control
- Combine with real-time threat information and Security Intelligence

## Expanded X-Force Threat Intelligence

- World-wide threat intelligence harvested by X-Force®
- Consumption of this data to make smarter and more accurate security decisions

## Security Intelligence Integration

- Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform



# Mobility: *Thinking through mobile security*

## At the Device

### Enroll

Register owner and services

### Configure

Set appropriate security policies

### Monitor

Ensure device compliance

### Reconfigure

Add new policies over-the-air

### De-provision

Remove services and wipe



Internet

## Over the Network and Enterprise

### Authenticate

Properly identify mobile users

### Encrypt

Secure network connectivity

### Monitor

Log network access and events

### Control

Allow or deny access to apps

### Block

Identify and stop mobile threats



Corporate Intranet

## For the Mobile App

### Develop

Utilize secure coding practices

### Test

Identify application vulnerabilities

### Monitor

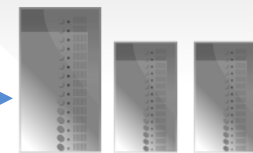
Correlate unauthorized activity

### Protect

Defend against application attacks

### Update

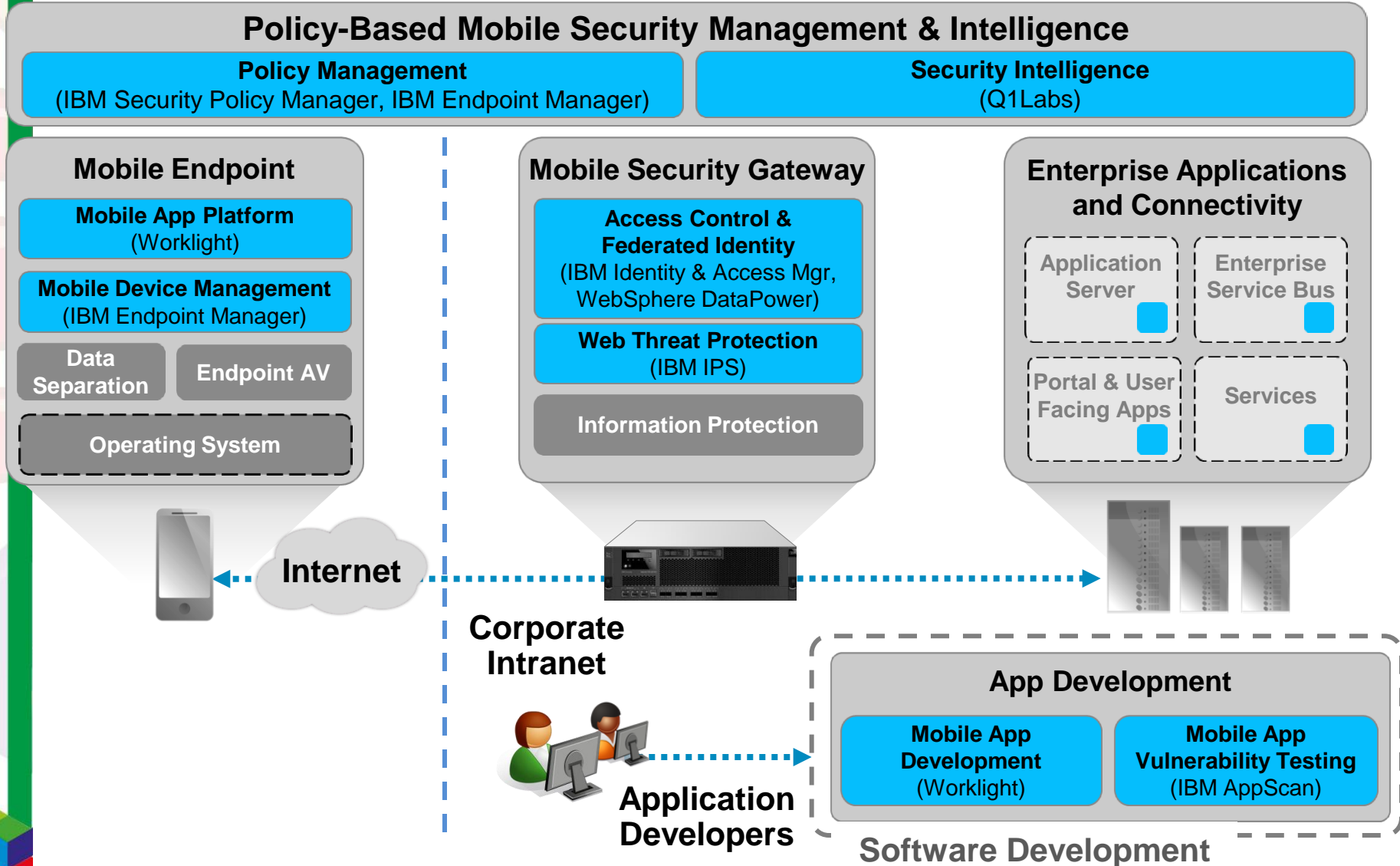
Patch old or vulnerable apps



## IBM Mobile Security Strategy

- Safe usage of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

# Mobility: *IBM's mobility capabilities today*



# Identity: IBM's IAM governance strategy and vision



## Integration with Threat and Security Intelligence

Expansion of IAM vertically through governance, analytics and reporting; Horizontal integration with additional security products and technologies

## Enhanced Identity Assurance

Improved built-in risk-based access control for cloud, mobile and SaaS access, as well as integration with proofing and validation solutions

## Insider Threat and IAM Governance

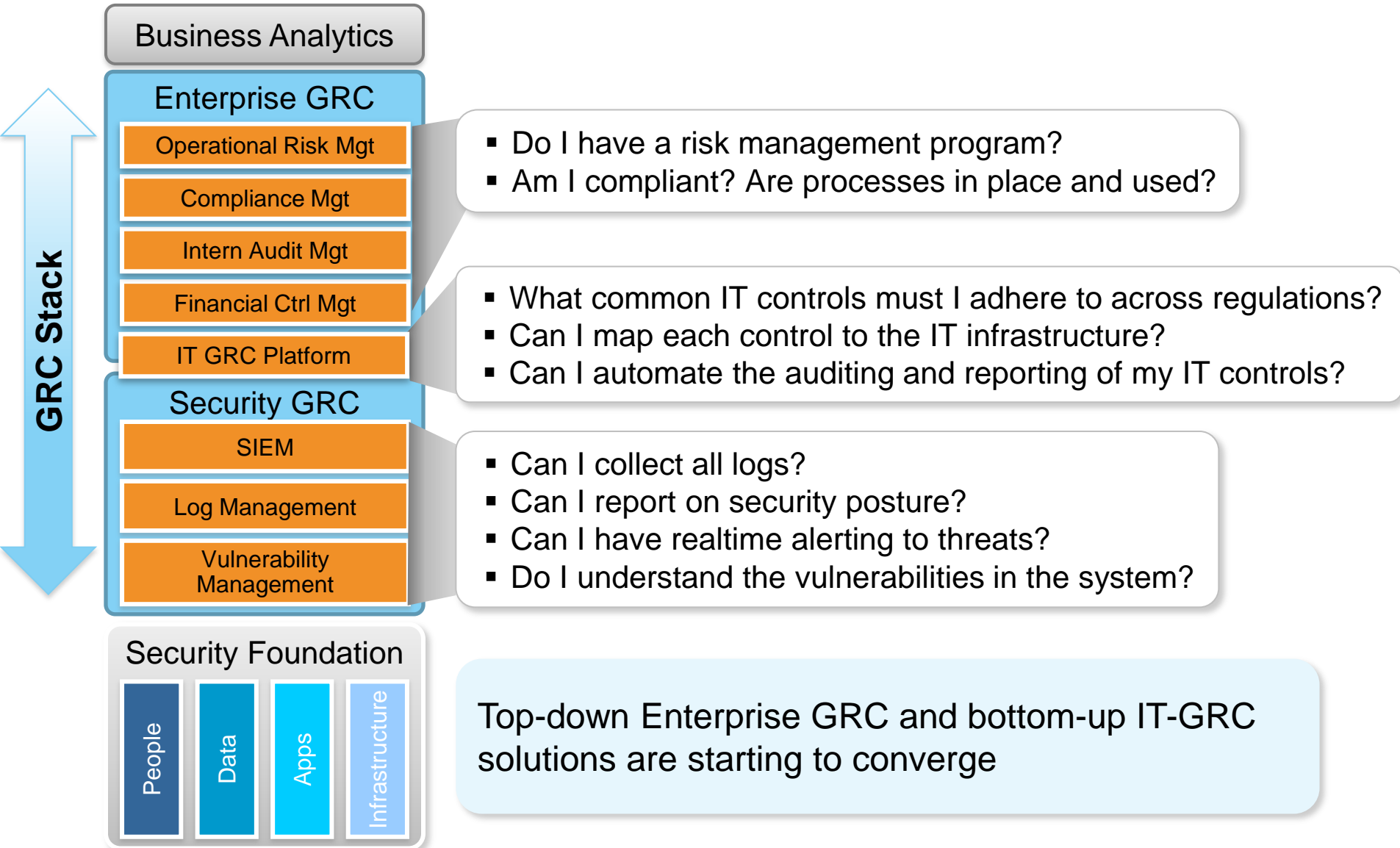
Further development of Privileged Identity Management (PIM) capabilities and enhanced Identity and Role Management

# Identity: IBM's IAM vision – product mapping



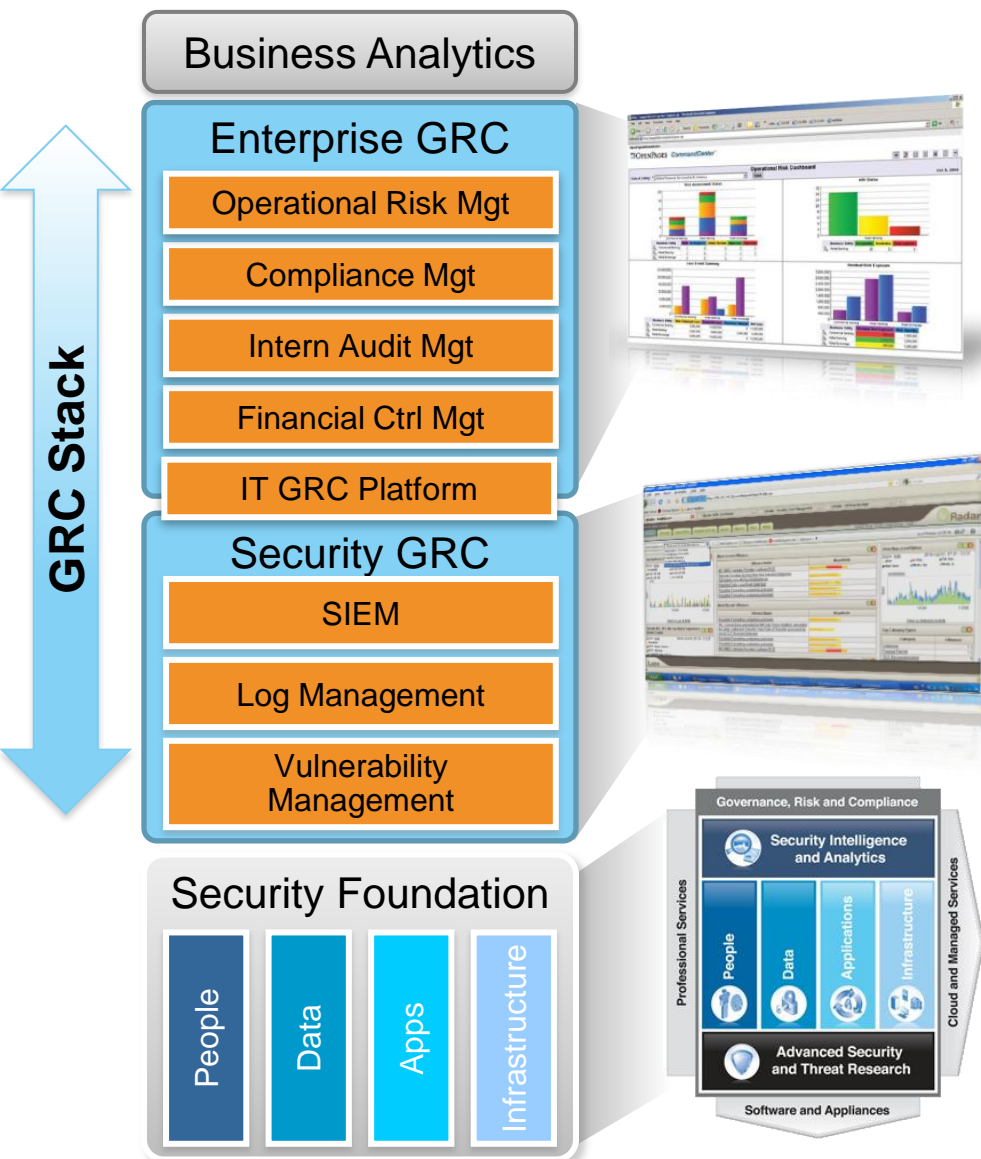
**Manage Enterprise Identity Context Across All Security Domains**

# GRC: Customers are looking for a stack of GRC capabilities





# GRC: *The GRC stack and IBM*



## OpenPages – Enterprise GRC Platform

- Driven by Enterprise Risk Management teams
- Focus on regulations such as SOX, HIPAA
- Focus is on Finance, Legal and Operational requirements
- Top down approach to requirements

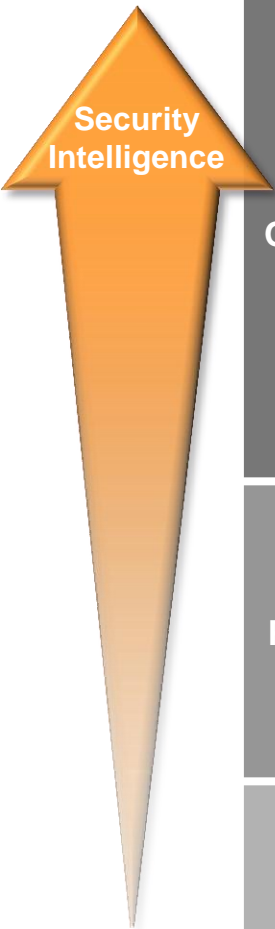
## QRadar SIEM and Risk Manager

- Driven by IT Security teams
- Focus on log collection, event analysis, and compliance reporting
- Focus on reducing IT security data to timely, relevant security information
- Bottom up approach to requirements

## IBM Security Portfolio

- Leading assets in (or 3<sup>rd</sup> party integrations with):
  - Identity management
  - Data security
  - Application security
  - Network and endpoint security

# Security Intelligence is enabling progress to optimized security



		<b>Security Intelligence:</b> Information and event management Advanced correlation and deep analytics External threat research			
Security Intelligence	Optimized	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Security rich systems
	Proficient	User provisioning Access management Strong authentication	Database activity monitoring Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset management Endpoint / network security management
	Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus
		People	Data	Applications	Infrastructure

# Helping define the new role of the information security leader and tracking security trends



## IBM CISO Study



<http://instituteforadvancedsecurity.com/content-library/m/files/97.aspx>

## IBM X-Force® Trend & Risk Report



[https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli\\_Organic&S\\_PKG=xforce-trend-risk-report](https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=xforce-trend-risk-report)



# IT Security must shift from a “defense-in-depth” mindset and begin thinking like an attacker



Off-the-Shelf  
tools and  
techniques

Sophisticated

## Audit, Patch & Block

*Think like a defender,  
defense-in-depth mindset*

- ✓ Protect all assets
- ✓ Emphasize the perimeter
- ✓ Patch systems
- ✓ Use signature-based detection
- ✓ Scan endpoints for malware
- ✓ Read the latest news
- ✓ Collect logs
- ✓ Conduct manual interviews
- ✓ Shut down systems

## Detect, Analyze, Remediate

*Think like an attacker,  
counter intelligence mindset*

- Protect high value assets
- Emphasize the data
- Harden targets and weakest links
- Use anomaly-based detection
- Baseline system behavior
- Consume threat feeds
- Collect everything
- Automate correlation and analytics
- Gather and preserve evidence

**Broad**

**Targeted**

A large, faint background graphic of stylized human figures in various colors (orange, yellow, green, blue, purple) holding hands in a circle. A vertical green bar is on the left side, and a colorful geometric shape is at the bottom left.

# Thank you!



# Acknowledgements, disclaimers and trademarks



© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, [ibm.com](http://ibm.com), Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

